(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 930 615 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.07.1999 Bulletin 1999/29

(51) Int. Cl.[6]: **G11B 20/10**, G11B 27/28

(21) Application number: **98112212.0**

(22) Date of filing: **02.07.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **20.01.1998 JP 891598**

(71) Applicant: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

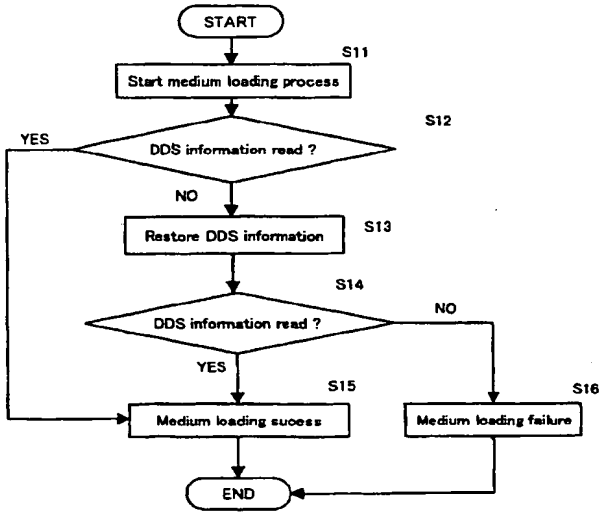
(72) Inventors:
- **Yamakawa, Teruji,**
  c/o Fujitsu Program Lab. Ltd.
  Yokohama, 222-0033 (JP)
- **Imamura, Kiyomi,**
  c/o Fujitsu Limited
  Kawasaki-shi, Kanagawa 211-8588 (JP)

(74) Representative:
Seeger, Wolfgang, Dipl.-Phys.
SEEGER & SEEGER
Patentanwälte & European Patent Attorneys
Georg-Hager-Strasse 40
81369 München (DE)

(54) Data storage device and control method therfor

(57) It is provided a data storage device which reads data from and/or writes data to a memory medium, comprising: an acquisition unit for acquiring management information which is recorded by a predetermined form in said memory; and a controller for converting the management information into an another form. The controller rearranges the management information to convert the management information into another form, and also the controller restores the converted management information to the predetermined form according to a relationship between a first identifier recorded on the memory medium and a second identifier recorded in the data storage device. When, for example, the two identifiers match, the acquisition unit can acquire the management information, and the reading and writing of data is enabled. When the two identifiers do not match, restoration of the management information to a predetermined form is not effected, so that the acquisition unit can not acquire the management information and the reading and writing of data is disabled.

FIG. 4



EP 0 930 615 A2

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates to a data storage device for recording data on a memory medium, such as a magneto-optical disk, and in particular to a data storage device which ensures the secrecy and the security of recorded data.

Related Arts

[0002] Generally, a data writable memory medium (hereinafter referred to as a medium), such as a magneto-optical disk (MO), can be inserted into or removed from a data storage device (hereinafter simply referred to as a storage device) which reads and writes predetermined data from and to the medium. When a medium is loaded into the storage device, operational control for the storage device is provided by commands issued by a superior apparatus, such as a personal computer connected to the storage device by a SCSI cable.

[0003] Conventionally, by taking compatibility into account, reading data from and writing data to a medium can also be performed by a storage device other than the device which was originally employed for writing data.

[0004] Fig. 19 is a flowchart for data reading/writing processing performed by a conventional storage device. After a medium is inserted into the storage device at step S1, at step S2 a process for loading the medium is started. That is, the medium is positioned at a predetermined location within the storage device and is rotated at a controlled revolution rate, and a process is performed to set the medium to a data reading enabled state or to a data writing enabled state. At step S3, medium information, such as configuration and memory capacity of the medium, are read, and at step S4 the reading and writing of data is enabled by the employment of an operation or a processing procedure based on the information.

[0005] Therefore, a problem has arisen in that once a memory medium has been acquired, secret data recorded on the memory medium, such as the contents of a client database or design data, can easily be stolen or altered.

SUMMARY OF THE INVENTION

[0006] It is, therefore, one objective of the present invention to provide a data storage device that ensures the secrecy and the security of data recorded on a memory medium.

[0007] To achieve the above objective, according to the present invention, a data storage device which reads data from and/or writes data to a memory medium, comprises:

an acquisition unit for acquiring management information which is recorded by a predetermined form in said memory,
a controller for converting said management information into an another form.

[0008] The controller rearranges the management information to convert the management information into another form; the controller shifts the management information by at least one bit to convert the management information into another form; or the controller encodes the management information to convert the management information into another form.

[0009] Further, the controller restores the converted management information to the predetermined form according to a relationship between a first identifier recorded on the memory medium and a second identifier recorded in the data storage device.

[0010] When, for example, the two identifiers match, the acquisition unit can acquire the management information, and the reading and writing of data is enabled. When the two identifiers do not match, restoration of the management information to a predetermined form is not effected, so that the acquisition unit can not acquire the management information and the reading and writing of data is disabled.

[0011] To achieve the above objective, according to the another present invention, a data storage device which reads data from and/or writes data to a memory medium, comprises:

an acquisition unit for acquiring management information which is recorded on a predetermined area of said memory medium,
a controller for moving said management information to an another area.

[0012] The acquisition unit acquires the moved management information from the another area according to a relationship between a first identifier recorded on the memory medium and a second identifier recorded in the data storage device.

[0013] For example,each the first and the second identifiers is a serial number for the data storage device and the predetermined area is a disk definition sector (DDS) area of the memory medium.

[0014] When, for example, the two identifiers match, the management information can be acquired from the another area, and the reading and writing of data is enabled. When the two identifiers do not match, and the acquisition unit does not acquire the management information because the acquisition unit tries to acquire the management information from the predetermined area where management information is not present, and the reading and the writing of data are disabled.

[0015] On the memory medium is recorded read

address information or write address information, which is used to control data reading or writing respectively. When the first and the second identifiers match, the controller may permit or inhibit the reading of data in accordance with the read address information or may permit or inhibit the writing of data in accordance with the write address information.

[0016] Preferably, provided for the memory medium is a first password. For example, when the reading of data is inhibited in accordance with read address information, if the first password matches a second password sent from a controller of the data storage device, the controller permits the reading of data.

[0017] The memory medium includes address information which designates at least one of a plurality of data sets which are recorded on the memory medium. For example, the controller may permit or inhibit the reading of data corresponding to the address information when both the first and the second identifiers match.

[0018] Other features and advantages of the present invention will become readily apparent from the following description when taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate presently preferred embodiments of the invention, and together with the general description given above and the detailed description of the preferred embodiments given below, serve to explain the principle of the invention, in which:

Fig. 1 is a block diagram illustrating a data storage device according to embodiments of the present invention;

Fig. 2 is a diagram showing an example layout of a disk format for a magneto-optical disk;

Fig. 3 is a specific diagram showing an example layout for a data area;

Fig. 4 is a flowchart for the security execution processing performed according to the embodiments of the present invention;

Fig. 5 is a flowchart for the security setup processing performed according to a first embodiment of the present invention;

Fig. 6 is a flowchart for the security execution processing performed according to the first embodiment of the present invention;

Fig. 7 is a diagram for explaining an example rearrangement of DDS information;

Fig. 8 is a flowchart for the security setup processing performed according to a second embodiment of the present invention;

Fig. 9 is a flowchart for the security execution processing performed according to the second embodiment of the present invention;

Fig. 10 is a flowchart for the security setup processing performed according to a third embodiment of the present invention;

Fig. 11 is a flowchart for the security execution processing performed according to the third embodiment of the present invention;

Fig. 12 is a diagram for explaining an example shift of DDS information;

Fig. 13 is a flowchart for the security setup processing performed according to a fourth embodiment of the present invention;

Fig. 14 is a flowchart for the security execution processing performed according to the fourth embodiment of the present invention;

Fig. 15 is a diagram showing the structure of a CDB for a security setup command that employs a vendor unique command;

Fig. 16 is a diagram showing the structure of a CDB for a format command the security level of which is designated;

Figs. 17A and 17B are diagrams depicting the structures of a parameter header and a level descriptor;

Figs. 18A and 18B are diagrams in each of which is shown the structure of a parameter field for a level descriptor; and

Fig. 19 is a flowchart showing the conventional processing performed when accessing a memory medium.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] The preferred embodiments of the present invention will now be described while referring to the accompanying drawings. However, the technical scope of the present invention is not limited to these embodiments. In the drawings, the same reference numerals or symbols are used to denote corresponding or identical components.

[0021] In the embodiment of the present invention, a magneto-optical disk (MO) is employed as the medium, but the medium that can be employed is not thereby limited, and another data writable memory medium, such as a CD-R, may be employed.

[0022] Fig. 1 is a schematic block diagram illustrating a magneto-optical disk device (data storage device) according to the present invention. In Fig. 1, a magneto-optical disk device 1 is connected via a SCSI interface to a personal computer 2, which is a control apparatus.

[0023] The magneto-optical disk device 1 comprises a mechanism controller 10, for performing the writing of data to and the reading of data from a magneto-optical disk, and a control unit which includes a magneto-optical disk controller (ODC) which employs firmware to implement a method according to the present invention.

[0024] The control unit further includes an MPU 12,

which controls the entire magneto-optical disk device 1; a D-RAM 13, which is a read/write buffer memory; a DSP 14, for performing positioning; a write data amplifier 14; a read data amplifier 16; an AGC amplifier 17; a head drive power amplifier 18; and a disk rotation motor controller 19.

[0025] The mechanism controller 10 includes a head sensor 100, a data reading/writing laser diode 101, and a detector 102 for detecting the inclination of a head. Further, the mechanism controller 10 includes a focus actuator 103, which is controlled by the head drive power amplifier 18; a track actuator 104; a disk ejection motor 105; a head drive voice coil motor 106; and a spindle motor 107, which is controlled by the motor controller 19, for rotating a disk.

[0026] When an operator enters a command (e.g., a read command or a write command) at a keyboard 3 of the personal computer 2, a SCSI command is transmitted by the computer 2 to the magneto-optical disk controller (ODC) 11 to start the writing/reading of data. Connected to the computer 2 is a display 4 on which data are displayed.

[0027] The magneto-optical disk controller (ODC) 11, which is provided with flash ROM for the storage of firmware, has an analysis function for analyzing SCSI commands received from the computer 2, and a coordination function for interacting with the MPU 12, in response to a SCSI command, to provide data writing/reading control for the mechanism controller 10.

[0028] The present invention can be applied not only for a SCSI command system but also for another command system, such as an ATA/ATAPI/SASI command system.

[0029] Fig. 2 is a diagram showing an example layout of a disk format for a magneto-optical disk (MO), i.e., the arrangement of areas on a 3.5-inch medium for a full RAM disk format conforming to ISO standards. As is shown in Fig. 2, in a range extending from a radius of 23.72 mm from the center of the MO disk to a radius of 41.00 mm is a data area in which user data can be written. The inside and the outside areas in the radial direction are medium information management areas in which are recorded various medium information, such as the type and the structure of a medium.

[0030] Fig. 3 is a specific diagram illustrating an example layout for the above data areas. In Fig. 3, the data areas are a user area, in which a user can write data, and DDS (Disk Definition Sector) areas, two of each being positioned on either side of the user area. In addition, a replacement area is provided for the user area as a spare area. The DDS areas are used to record management information of the medium (hereinafter referred to as DDS information), which is information for managing the user area, for example, information for a defect in the user area.

[0031] When the storage device is to access the medium for the reading or the writing of data, first, the ODC 11 reads the DDS information, and then, after the DDS information have been effectively acquired, accessing the user area is possible. Therefore, if the acquisition of DDS information fails for a specific reason, accessing the user area is not possible. In other words, the reading and writing of data to the medium is disabled.

[0032] In the preferred embodiments of the present invention, the acquisition of DDS information by the ODC 11 is disabled under a predetermined condition in order to inhibit access of the user area and thus ensure the security of the data recorded in the user area.

[0033] Specifically, in response to a specific security setup command issued by the personal computer 2 connected to the storage device, the ODC 11 performs security processing for the conversion of DDS information, which are recorded in a predetermined area on a medium and in a predetermined form, into another form, or for recording the DDS information in another area. When the DDS information are converted into an another form from the predetermined form, to ensure security DDS information having a specific form are not copied to an another area on the medium. However, DDS information having the specific form may be copied to an another area. The specific form may be a format standard defined by the ISO, for example.

[0034] When a medium whereon DDS information have been converted into an another form or have been moved and recorded in an another area is inserted into a storage device, the ODC 11 can not acquire the DDS information, and loading of the medium fails. However, if a process for restoring the original form from its current, converted form, or a process for reading DDS information to another area is performed, the DDS information can be effectively acquired.

[0035] Fig. 4 is a flowchart for the security execution processing performed in the preferred embodiments of the present invention. In Fig. 4, when a medium loading process is started at step S11 the process for reading of DDS information is performed (step S12), i.e., DDS information having a predetermined form which are recorded in the DDS area are read. When, as described above, the ODC 11 has not performed a security process for converting the DDS information into another form, or for storing the DDS information in another area, the DDS information can be effectively read, and the medium loading process is successful (step S15). When the security process has been performed, a process for restoring DDS information, or a process for reading DDS information to an another area, which will be described later, is performed (step S13). If the DDS information have effectively been obtained, the loading of the medium is successful (step S15). When the DDS information can not be restored or the DDS information have been destroyed, the DDS information can not be obtained and the loading of the medium fails (step S16). When the loading of the medium is successful, an identifier and address information, which will be described later, may be examined, and whether or not access has

been enabled may be checked.

[0036] In addition, in the preferred embodiments of the present invention, during the security processing an identifier of a storage device is recorded in a predetermined area of a medium. Then, as is described above, when the DDS information have been converted into another form, or have been moved and recorded in an another area, and the medium on which the identifier has been recorded is inserted into a specific storage device, the ODC 11 restores the DDS information having a predetermined form, or reads the DDS information from the current area only when the identifier of the storage device matches the identifier recorded on the medium. As a result, accessing the user area is enabled, and the reading and the writing of data can be performed.

[0037] When the two identifiers do not match, the DDS information having a predetermined form can not be restored, and the current form of the data is not altered, so that the DDS information can not effectively be acquired. When, under the same condition, the DDS information have been moved to an another area, the DDS area is cleared and initialized, so that the ODC 11 can not read and effectively obtain the DDS information from the DDS area. Therefore, access of the user area is inhibited. As described above, since a storage device that has an identifier differing from that written on the medium is prevented from reading and writing data relative to the medium, the security of data is ensured.

[0038] A more specific description of the preferred embodiments of the present invention will now be given. Figs. 5 and 6 are flowcharts for explaining a first embodiment of the present invention. The flowcharts, which are explained below, are for the processing performed by the ODC 11.

[0039] Fig. 5 is a flowchart for the security setup processing performed according to the first embodiment of the present invention. In Fig. 5, at step S101 the ODC 11 receives a security setup command, which will be described later, from the computer 2, which is a control apparatus. At step S102, upon the receipt of the security setup command, the ODC 11 converts into an another form DDS information which have a predetermined form and which are recorded in a DDS area in Fig. 3. As a result, the DDS information are rearranged as is described below.

[0040] Fig. 7 is a diagram for explaining an example rearrangement of DDS information. In Fig. 7, the DDS area is divided into segments of one byte each, and the individual segments are numbered. If, for example, DDS information are Chinese character data, such that one character consists of two bytes, the positions of the bytes in each byte pair in the DDS area are inverted, as is shown in Fig. 7.

[0041] After the DDS information recorded in a predetermined form in a DDS area have been rearranged, the ODC 11 can not effectively acquire the DDS information when it attempts to read the data as it was originally recorded.

[0042] Referring again to Fig. 5, at step S103 the rearranged DDS information are recorded in the DDS area, and at step S104, in addition to the rearrangement of the DDS information, the ODC 11 records the identifier of the storage device, into which the medium is inserted, and a security flag in a predetermined area on the medium. The identifier of the storage device is recorded in the flash ROM provided for the ODC 11. The security flag is data indicating whether security data have been set. When the security flag is set ON, in accordance with the security setup command, the security data have been set. When the security flag is set to OFF, the security data have not been set. A predetermined area in which the security flag and the identifier are recorded may be at a location designated in the DDS area in advance, or at a location outside the DDS area.

[0043] Fig. 6 is a flowchart showing the security execution processing performed according to the first embodiment of the present invention. In Fig. 6, at step S111, the medium is inserted into the storage device and a process for loading the medium is started. Specifically, a process for enabling the reading and the writing of data is begun.

[0044] At step S112, the data for the security flag are read from the predetermined area on the medium. When the security flag is OFF (no security setup effected), it is assumed that the above described data rearrangement in the DDS area has not been performed, and the DDS information can be effectively acquired. Therefore, accessing the user area is possible, and the loading of the medium is successful (step S113). In other words, the reading and the writing of data are possible.

[0045] When, at step S112, the security flag is ON (security setup effected), at step S114 the identifier recorded on the medium is compared with the identifier of the storage device into which the medium has been inserted. When the two identifiers match, DDS information having a predetermined form can be restored before being read (step S115). The DDS information can be normally acquired, so that the loading of the medium is successful (step S116). If, at step S114, the two identifiers do not match, the DDS information having a predetermined form can not be restored before reading, and the DDS information which have been rearranged in an another form are read. Thus, the DDS information can not be effectively acquired, and the loading of the medium fails (step S117). In other words, the reading and the writing of data are disabled.

[0046] When a medium is inserted into a storage device which does not support the security setup command, the examination of the security flag and the comparison of the identifiers are not performed, and the reading of DDS information is started. However, since the DDS information have been rearranged in an another form, the DDS information can not be effectively obtained, and the loading of the medium fails.

[0047] In the first embodiment, when the security setup command is transmitted by the control apparatus, the identifier of the storage device and the security flag are recorded in a predetermined area on the medium. When the medium is inserted into a storage device and the identifier of the storage device does not match the identifier recorded on the medium, the DDS information having a predetermined form can not be restored to their original form, and the DDS information can not be effectively acquired. Therefore, the user area can not be accessed and the reading and the writing of data are disabled, so that the secrecy and the security of data are thereby ensured.

[0048] Figs. 8 and 9 are flowcharts for explaining a second embodiment of the present invention. Fig. 8 is a flowchart showing the security setup processing performed according to the second embodiment. In fig. 8, at step S201 the ODC 11 receives a security setup command from the computer 2, which is a control apparatus. At step S202, upon the receipt of the security setup command, the ODC 11 reads the DDS information recorded in the DDS area in Fig. 3. At step S203, the ODC 11 moves the DDS information to another area. For example, the DDS information may be moved to a replacement area shown in Fig. 3. In other words, the DDS information are recorded in the replacement area and the DDS information in the DDS area are deleted.

[0049] At step S204, as well as in the first embodiment, in addition to the moving of the DDS information, the ODC 11 records in a predetermined area on the medium the identifier of the storage device into which the medium is inserted and the security flag.

[0050] Fig. 9 is a flowchart showing the security execution processing performed according to the second embodiment of the present invention. In Fig. 9, at step S211 the medium is inserted into the storage device and a process for loading the medium is started. Specifically, a process for enabling the reading and the writing of data is begun.

[0051] At step S212, data for the security flag are read from the predetermined area on the medium. When the security flag is OFF (no security setup effected), it is assumed that the above described movement from the DDS area has not been performed, and the DDS information can be effectively acquired. Therefore, accessing the user area is possible, so that the loading of the medium is successful (step S213). In other words, the reading and the writing of data are possible.

[0052] When, at step S212, the security flag is ON (security setup effected), at step S214 the identifier recorded on the medium is compared with the identifier of the storage device into which the medium has been inserted. When the two identifiers match, the ODC 11 assumes that the DDS information are recorded in the replacement area, and reads the DDS information from the replacement area (step S215). The DDS information are normally acquired, and the loading of the medium is successful (step S216). If, at step S214, the two identifiers do not match, the ODC 11 assumes that the DDS information are recorded in the DDS area, and tries to read the DDS information from the DDS area (step S217). However, as is described above, since the DDS information in the DDS area have been deleted, the ODC 11 can not acquire the data and the loading of the medium fails (step S218). In other words, the reading and the writing of data are disabled.

[0053] When a medium is inserted into a storage device for which the security setup command is not supported, the examination of the security flag and the comparison of the identifiers are not performed, and the reading of DDS information is started. However, since the DDS information have been deleted from the DDS area, the DDS information can not be effectively obtained and the loading of the medium fails.

[0054] In the second embodiment, when the security setup command is transmitted by the control apparatus, the identifier of the storage device and the security flag are recorded in a predetermined area on the medium. When the medium is inserted into a storage device and the identifier of the storage device does not match the identifier recorded on the medium, the device attempts to read the DDS information from the DDS area wherein the DDS information were deleted, but the DDS information can not be effectively acquired. Therefore, the user area can not be accessed and the reading and the writing of data are disabled, so that the secrecy and the security of data are thereby ensured.

[0055] Figs. 10 and 11 are flowcharts for explaining a third embodiment of the present invention. Fig. 10 is a flowchart showing the security setup processing performed according to the third embodiment. In fig. 10, at step S301 the ODC 11 receives a security setup command, which will be described later, from the computer 2, which is a control apparatus. At step S302, upon the receipt of the security setup command, the ODC 11 shifts the DDS information recorded in the DDS area in Fig. 3 by at least one bit.

[0056] Fig. 12 is a diagram for explaining an example shift of the DDS information. As is shown in Fig. 12, the DDS information of 8 bits are shifted by one bit in the DDS area, the last bit (08) being moved to the first bit position. In other words, bit rotation is performed. When DDS information having a predetermined form which are recorded in the DDS area are shifted, the ODC 11 can not effectively acquire the DDS information when it attempts to read the data as it was originally recorded.

[0057] At step S303, the shifted DDS information are recorded in the DDS area. At step S304, as well as in the first embodiment, in addition to shifting of the DDS information, the ODC 11 records the identifier of the storage device into which the medium has been inserted and the security flag in a predetermined area on the medium.

[0058] Fig. 11 is a flowchart showing the security execution processing performed according to the third embodiment of the present invention. In Fig. 11, at step

S311 the medium is inserted into the storage device and a process for loading the medium is started. Specifically, a process for enabling the reading and the writing of data is begun.

[0059] At step S312, data for the security flag are read from the predetermined area on the medium. When the security flag is OFF (no security setup effected), it is assumed that the above described shifting of the DDS information in the DDS area has not been performed, and the DDS information are effectively acquired. Therefore, accessing the user area is possible, so that the loading of the medium is successful (step S313). In other words, the reading and the writing of data are possible.

[0060] When, at step S312, the security flag is ON (security setup effected), at step S314 the identifier recorded on the medium is compared with the identifier of the storage device into which the medium is inserted. When the two identifiers match, the DDS information are restored to their original form before being read (step S315). The DDS information are normally acquired, and the loading of the medium is successful (step S316). If, at step S314, the two identifiers do not match, the DDS information are not restored to their original form, and the DDS information which have been shifted are read. As a result, the ODC 11 can not acquire the DDS information and the loading of the medium fails (step S317). In other words, the reading and the writing of data are disabled.

[0061] When a medium is inserted into a storage device for which the security setup command is not supported, the examination of the security flag and the comparison of the identifiers are not performed, and the reading of the DDS information is started. However, since the DDS information have been shifted in the DDS area, the DDS information can not be effectively obtained and the loading of the medium fails.

[0062] In the third embodiment, when the security setup command is transmitted by the control apparatus, the identifier of the storage device and the security flag are recorded in a predetermined area on the medium. When the medium is inserted into a storage device and the identifier of the storage device does not match the identifier recorded on the medium, the DDS information that have been shifted are not restored to their original form and the DDS information can not be effectively acquired. Therefore, the user area can not be accessed and the reading and the writing of data are disabled, so that the secrecy and the security of the data are thereby ensured.

[0063] Figs. 13 and 14 are flowcharts for explaining a fourth embodiment of the present invention. Fig. 13 is a flowchart showing the security setup processing performed according to the fourth embodiment. In Fig. 13, at step S401 the ODC 11 receives a security setup command from the computer 2, which is a control apparatus. At step S402, upon the receipt of the security setup command, the ODC 11 encodes the DDS information recorded in the DDS area in Fig. 3. For example, the encoding in performed by cipherring. The encoding of data is performed by using, for example, predetermined encode/decode, or cipher/decipher software provided for the ODC 11.

[0064] At step S403, the encoded DDS information are recorded in the DDS area. At step S404, as well as in the first embodiment, in addition to encoding the DDS information, the ODC 11 records the identifier of the storage device into which the medium is inserted and the security flag in a predetermined area on the medium.

[0065] Fig. 14 is a flowchart showing the security execution processing performed according to the fourth embodiment of the present invention. In Fig. 14, at step S411 the medium is inserted into the storage device and a process for loading the medium is started. Specifically, a process for enabling the reading and the writing of data is begun.

[0066] At step S412, data for the security flag are read from the predetermined area on the medium. When the security flag is OFF (no security setup effected), it is assumed that the above described shifting of the DDS information in the DDS area has not been performed, and the DDS information are effectively acquired. Therefore, accessing the user area is possible, and the loading of the medium is successful (step S413). In other words, the reading and the writing of data are possible.

[0067] When, at step S412, the security flag is ON (security setup effected), at step S414 the identifier recorded on the medium is compared with the identifier of the storage device into which the medium is inserted. When the two identifiers match, before being read, the DDS information are decoded by the predetermined encode/decode software provided for the ODC 11, and the DDS information are restored to their original form (step S415). Thus, the DDS information are normally acquired, and the loading of the medium is successful (step S416). If, at step S414, the two identifiers do not match, the DDS information are read without being decoded. As a result, the ODC 11 can not acquire the DDS information and the loading of the medium fails (step S417). In other words, the reading and the writing of data are disabled.

[0068] When a medium is inserted into a storage device for which the security setup command is not supported, the examination of the security flag and the comparison of the identifiers are not performed, and the reading of DDS information is started. However, since the DDS information have been encoded, the DDS information can not be effectively obtained and the loading of the medium fails.

[0069] In the fourth embodiment, when the security setup command is transmitted by the control apparatus, the identifier of the storage device and the security flag are recorded in a predetermined area on the medium. When the medium is inserted into a storage device and

the identifier of the storage device does not match the identifier recorded on the medium, the DDS information are read without being decoded, and the DDS information can not be effectively acquired. Therefore, the user area can not be accessed, the reading and writing of data is disabled, and the secrecy and the security of data are thereby ensured.

[0070] Fig. 15 is a diagram showing an example CDB (Command Descriptor Block) for a security setup command which is transmitted by the personal computer 2 to the storage device 1. The security setup command in Fig. 15 is prepared by using a vender unique command for the SCSI interface. As is described above, the security setup data, according to which memory medium access is permitted only when the identifier recorded on a memory medium matches the identifier of a storage device, are set to the security level established by the security setup command.

[0071] The security level may be designated in accordance with a normal format command, instead of the security setup command being set by using the vender unique command. Fig. 16 is a diagram showing an example CDB for a format command for which the security level is set by using the SCSI command.

[0072] In the individual embodiments, the security is released when the identifier recorded on the medium matches the identifier of the storage device into which the medium is inserted. To enhance the secrecy of data, a security function for restricting the reading and the writing of data may be additionally provided.

[0073] Thus, read address information and write address information are recorded in the parameter head of a parameter, which is designated by the security setup command (Fig. 15) or the format command (Fig. 16) for which the security level has been set.

[0074] Figs. 17A and 17B are diagrams showing an example structure for a parameter designated by the above commands. The parameter is constituted by a parameter head, shown in Fig. 17A, and a level descriptor, shown in Fig. 17B. The read and write address information are written in the parameter head in Fig. 17A. The read address information and the write address information are recorded in a predetermined area, in addition to the security address information which is recorded during the security setup process performed in the above embodiments.

[0075] The level descriptor in Fig. 17B consists of a header of two bytes and a succeeding parameter field. The parameter field is divided into units called pages, in which are recorded individual function attributes. The password is recorded in the level descriptor in the parameter.

[0076] Fig. 18A is a diagram showing a page for passwords in the parameter field (see Fig. 17B) of the level descriptor. The password is written in the security area together with the read and write address information. Fig. 18B is a diagram in which pages, shown in the parameter field of the level descriptor, are designated for the recording of a logical block addresses (LBAs), which will be described later.

[0077] When, for example, the read address information have not been set, the reading of data is permitted. But when the read address information have been set, the reading of data is inhibited even though the identifiers match. However, if a predetermined password from the computer 2 is input at this time, the reading of data is permitted.

[0078] And when, for example, the write address information have not been set, the writing of data is permitted. But when the write address information have been set, the writing of data is inhibited even though the identifiers match. However, if a predetermined password from the computer 2 is input at this time, the writing of data is permitted.

[0079] Further, in the above embodiments, all the data recorded on the medium are objects for which the setting of security is performed. When a plurality of data sets are recorded on the medium, however, the setting of security is desired for only a part of those data.

[0080] Therefore, to set the security for the medium, a logical block address (LBA) for selected data is designated in the level descriptor of the parameter in Fig. 15. More specifically, a LBA designation page for designating data for which security is to be set is entered in a parameter field of the level descriptor (see Fig. 18B). The LBA is an address for a predetermined unit of data recorded in the user area in Fig. 3. As is shown in Fig. 18B, for setting security a data LBA (security LBA) having a length of three bytes, for example, is designated. The data for the security LBA are recorded in a predetermined area at the same time as the identifier of the storage device is recorded therein.

[0081] As a result, even when the identifiers match and the security is released, only the reading and writing of data that correspond to the LBA entered in the LBA designation page is permitted. In addition, even when the read address information or the write address information have been set and reading or writing is permitted, only the reading and writing of data that correspond to the LBA entered in the LBA designation page is permitted.

[0082] A storage device, such as a DVD player, which incorporates a processor serving as a host computer, can perform the above security process internally.

[0083] As is described above, according to the present invention, the form of DDS information recorded on a medium may be altered in response to a security setup command, which is transmitted by a control apparatus (personal computer) to control a data storage device. Then, when the medium is inserted into a storage device and the identifier of the storage device does not match the identifier recorded on the medium, the reading of the DDS information in its altered form is started, so that the DDS information can not be effectively obtained. Therefore, the user area can not be accessed and the reading and the writing of data are

disabled. And in the event the medium was stolen, the secrecy and the security of data recorded on the medium are ensured.

[0084] The present invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The present embodiment is therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than by foregoing description and all change which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

Claims

1. A data storage device for reading data from and/or writing data to a memory medium, comprising:

   an acquisition unit for acquiring management information which is recorded by a predetermined form in said memory; and
   a controller for converting said management information which is recorded by a predetermined form in said memory medium into an another form.

2. The data storage device according to claim 1, wherein said controller rearranges said management information to convert said management information into said another form.

3. The data storage device according to claim 1, wherein said controller shifts said management information by at least one bit to convert said management information into said another form.

4. The data storage device according to claim 1, wherein said controller encodes said management information to convert said management information into said another form.

5. The data storage device according to claim 1, wherein said controller restores said converted management information to said predetermined form according to a relationship between a first identifier recorded on said memory medium and a second identifier recorded in said data storage device.

6. The data storage device according to claim 5,

   wherein access control information for controlling an access to at least one of a plurality of said data is recorded on said memory; and
   said controller permits or inhibits accessing of said designated data according to relationship between said first identifier and said second identifier.

7. The data storage device according to claim 5,

   wherein read access control information for controlling a read access to said data is recorded on said memory medium; and
   said controller permits or inhibits reading of said data according to said read address information and relationship between said first identifier and said second identifier.

8. The data storage device according to claim 5,

   wherein read access control information said data and access control information which designates at least one of a plurality of said data are recorded on said memory medium; and
   said controller permits or inhibits reading of said designated data according to said read address information and relationship between said first identifier and said second identifier.

9. The data storage device according to claim 5, wherein read access control information said data and a first password are recorded on said memory medium;

   said controller permits or inhibits reading of said data according to said read address information, relationship between said first password and an inputted second password and relationship between said first identifier and said second identifier.

10. The data storage device according to claim 5,

    wherein write access control information for controlling a write access to said data is recorded on said memory medium; and
    said controller permits or inhibits writing of said data according to said write address information and relationship between said first identifier and said second identifier.

11. The data storage device according to claim 5,

    wherein write access control information for controlling a write access to said data and access control information which designates at least one of a plurality of said data are recorded on said memory medium; and
    said controller permits or inhibits writing of said designated data according to said write address information and relationship between said first identifier and said second identifier.

12. The data storage device according to claim 5, wherein write access control information for controlling write access to said data and a first password

are recorded on said memory medium;

said controller permits or inhibits writing of said data according to said write access control information, relationship between said first password and an inputted second password and relationship between said first identifier and said second identifier.

13. The data storage device according to claim 5,

wherein each said first and said second identifiers is a serial number for said data storage device.

14. The data storage device according to claim 1,

wherein said memory medium is a disk which is removable from said data storage device.

15. The data storage device according to claim 14,

wherein said disk is a magneto-optical disk; and
said predetermined area is a disk definition sector (DDS) area in which management information for said memory medium is recorded.

16. A data storage device which reads data from and/or writes data to a memory medium, comprising:

an acquisition unit for acquiring management information which is recorded on a predetermined area of said memory; and
a controller for moving said management information to an another area.

17. The data storage device according to claim 16, wherein said acquisition unit acquires said moved management information from said another area according to a relationship between a first identifier recorded on said memory medium and a second identifier recorded in said data storage device

18. A method for controlling a data storage device which reads data from and/or writes data to a memory medium, comprising the steps of:

acquiring management information which is recorded by a predetermined form in said memory; and
converting said management information of said memory medium into an another form.

19. The method for controlling a data storage device according to claim 18, wherein, at said converting step, said management information is rearranged to convert said management information into said another form.

20. The method for controlling a data storage device according to claim 18, wherein, at said converting step, said management information is shifted by at least one bit to convert said management information into said another form.

21. The method for controlling a data storage device according to claim 18, wherein, at said converting step, said management information is encoded to convert Said management information into said another form.

22. The method for controlling a data storage device according to claim 18, further comprising the steps of:

restoring said converted management information to said predetermined form according to a relationship between a first identifier recorded on said memory medium and a second identifier recorded in said data storage device; and
acquiring said restored management information.

23. A control method for a data storage device which reads data from and/or writes data to a memory medium, comprising the steps of:

acquiring management information which is recorded on a predetermined area of said memory; and
moving said management information of said memory medium to another area in said memory medium.

24. The method for controlling a data storage device according to claim 23, further comprising the step of:

acquiring said moved management information from said another area according to a relationship between a first identifier recorded on said memory medium and a second identifier recorded in said data storage device.

FIG. 1

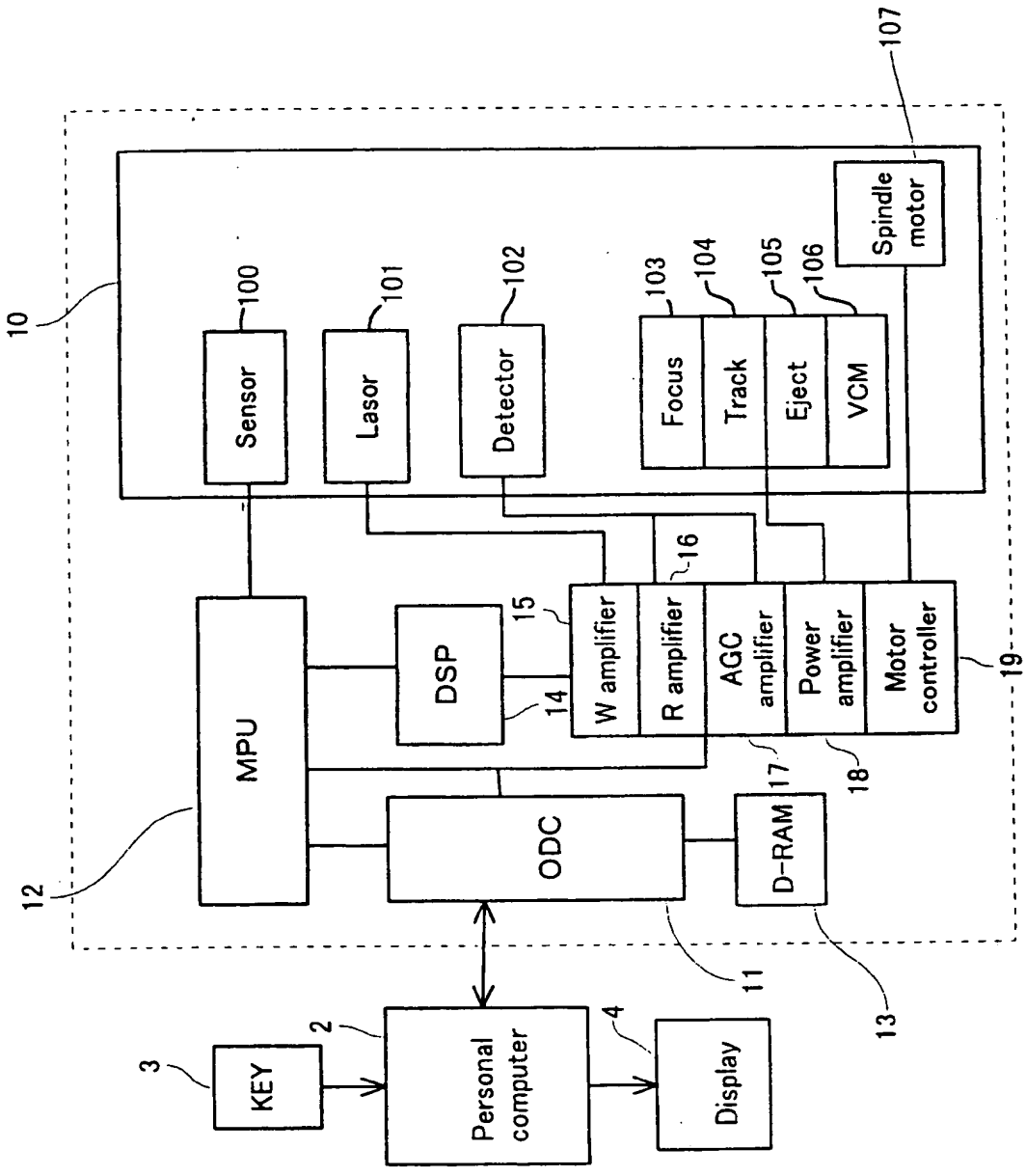


FIG. 2

	Zone	Radius mm	Track No.
Medium information management area	Lead-in Zone		
	Initial Zone	22.60～23.14	
	Acquire Zone		
	Lead-in tracks	23.14～23.60	-434～-93
	Focus tracks	23.60～23.61	-88～-85
	Inner Test Zone		
	for manufacturers	23.61～23.65	-84～-53
	for drives	23.65～23.70	-52～-21
	Inner Control Zone	23.70～23.72	-20～-5
	Buffer Zone	23.72～23.72	-4～-1
Data area	Data Zone	23.72～41.00	0～18479
Medium information management area	Outer Test Zone		
	for manufacturers	41.00～41.02	18480～18511
	for drives	41.02～41.06	18512～18543
	Buffer Zone	41.06～41.28	18544～18854

FIG. 3

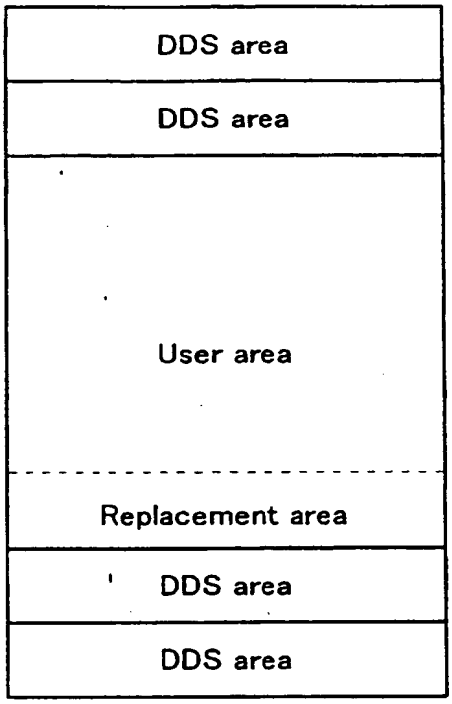


FIG. 4

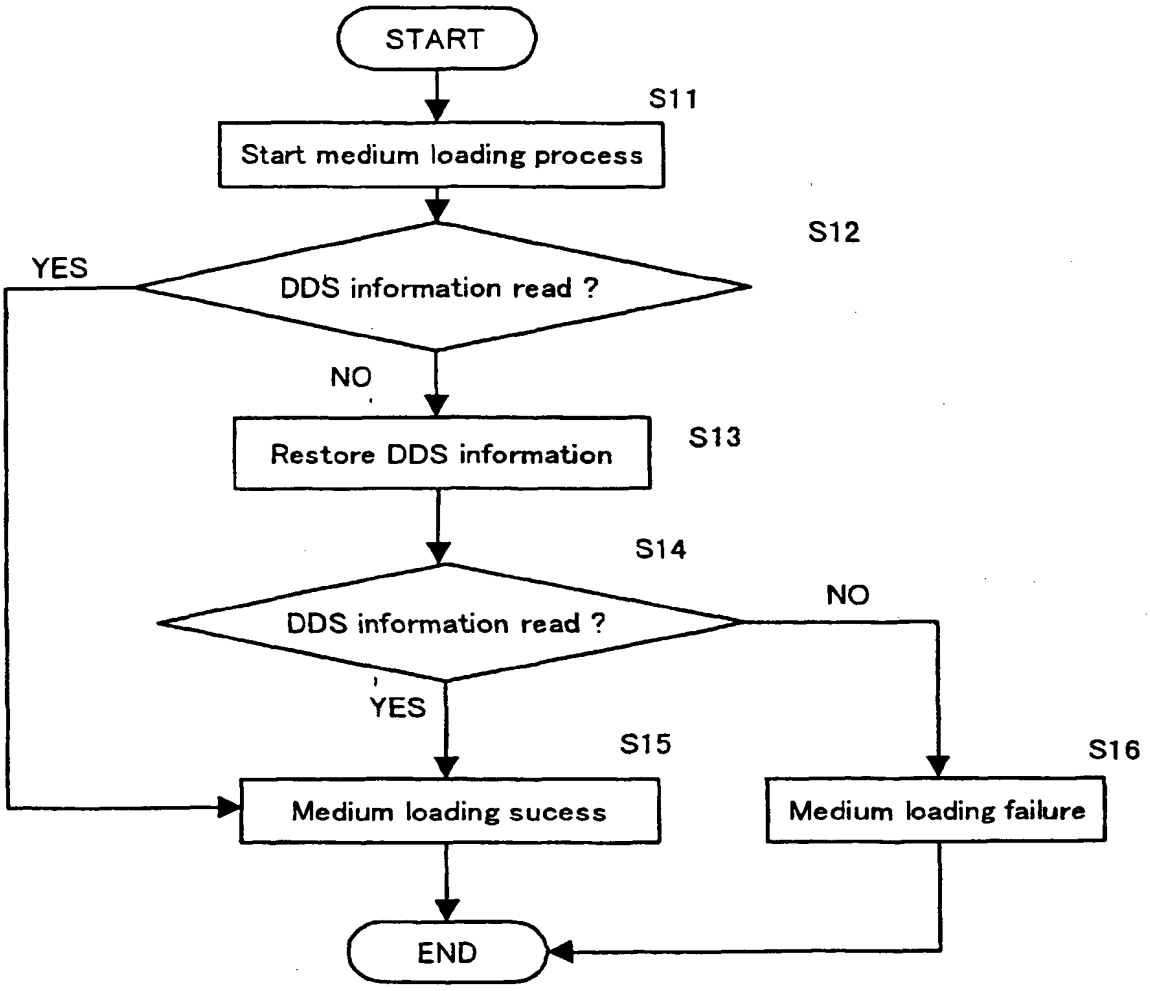


FIG. 5

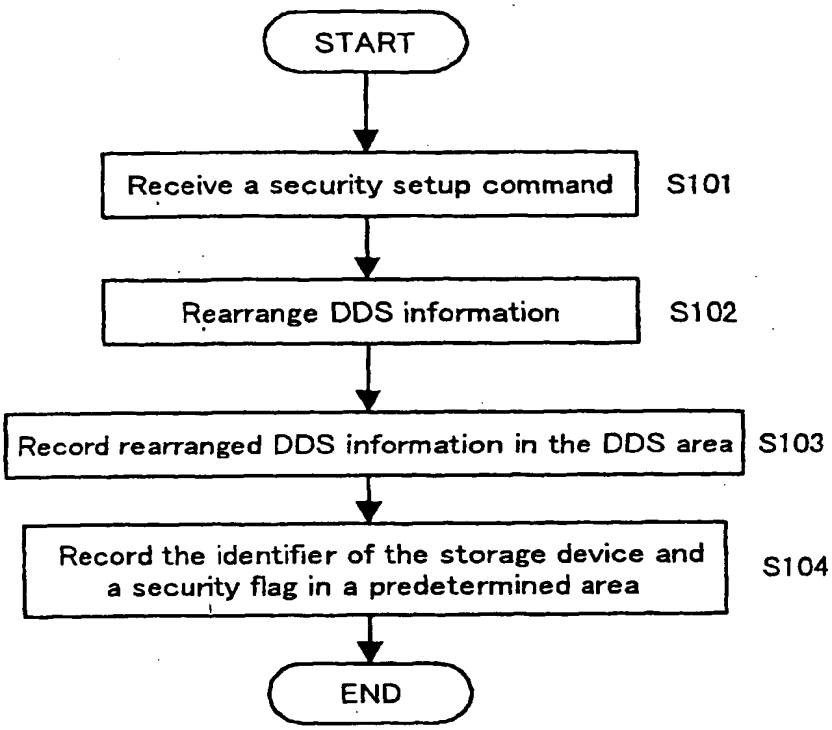


FIG. 6

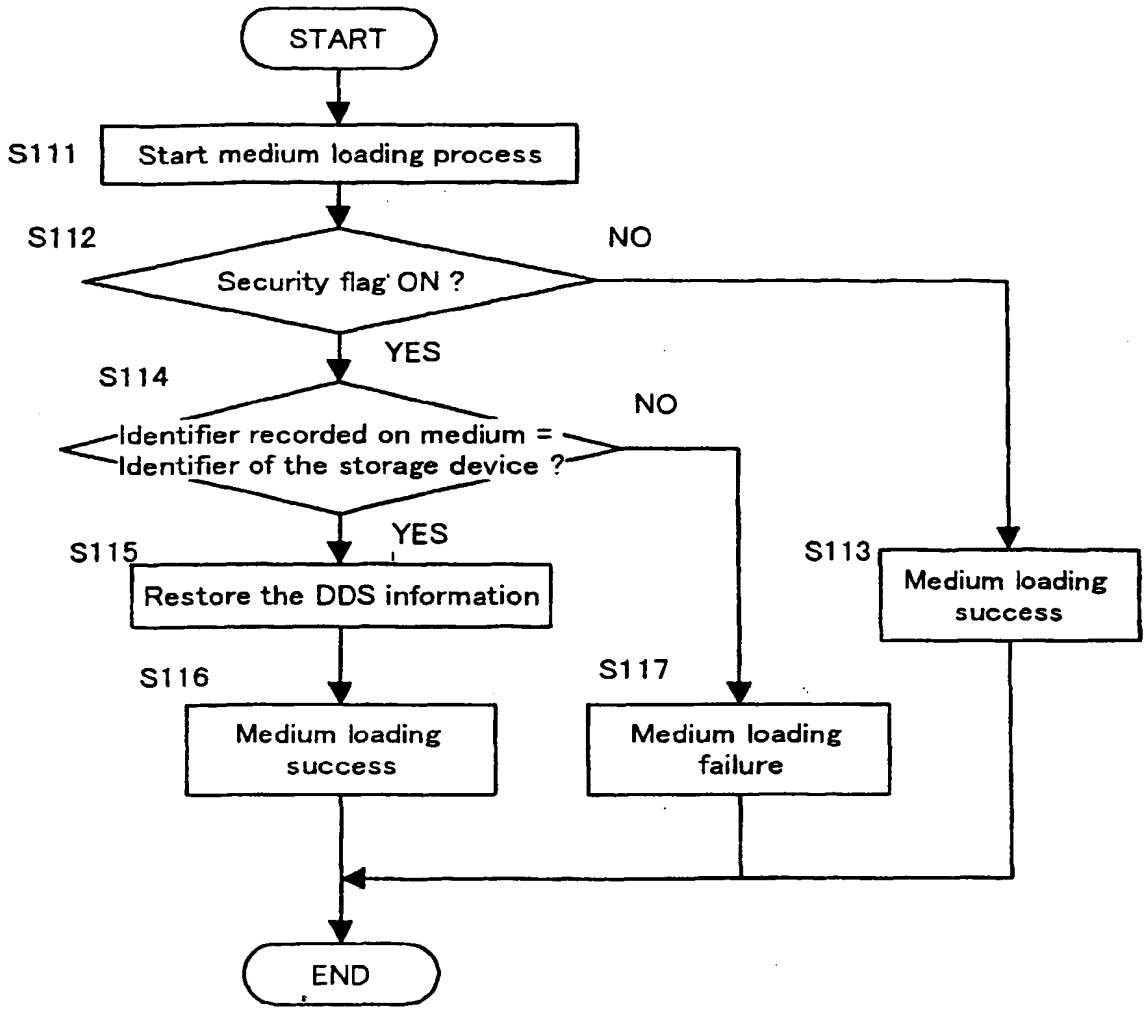


FIG. 7

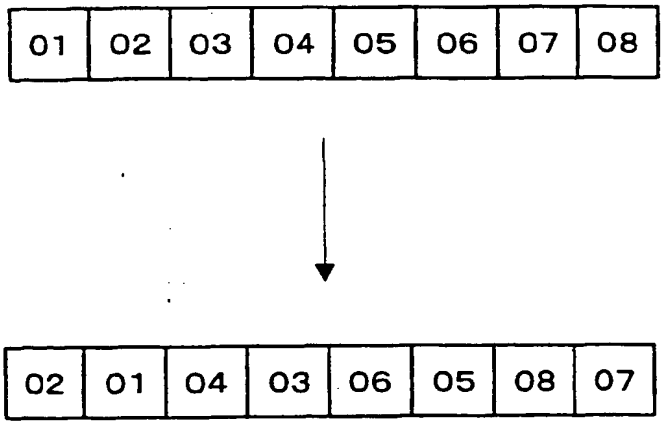


FIG. 8

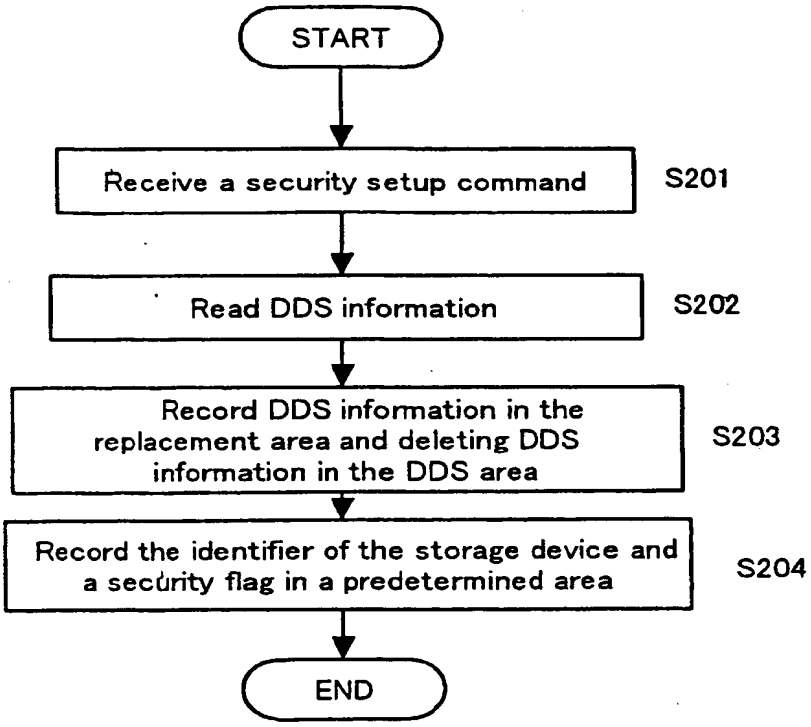


FIG. 9

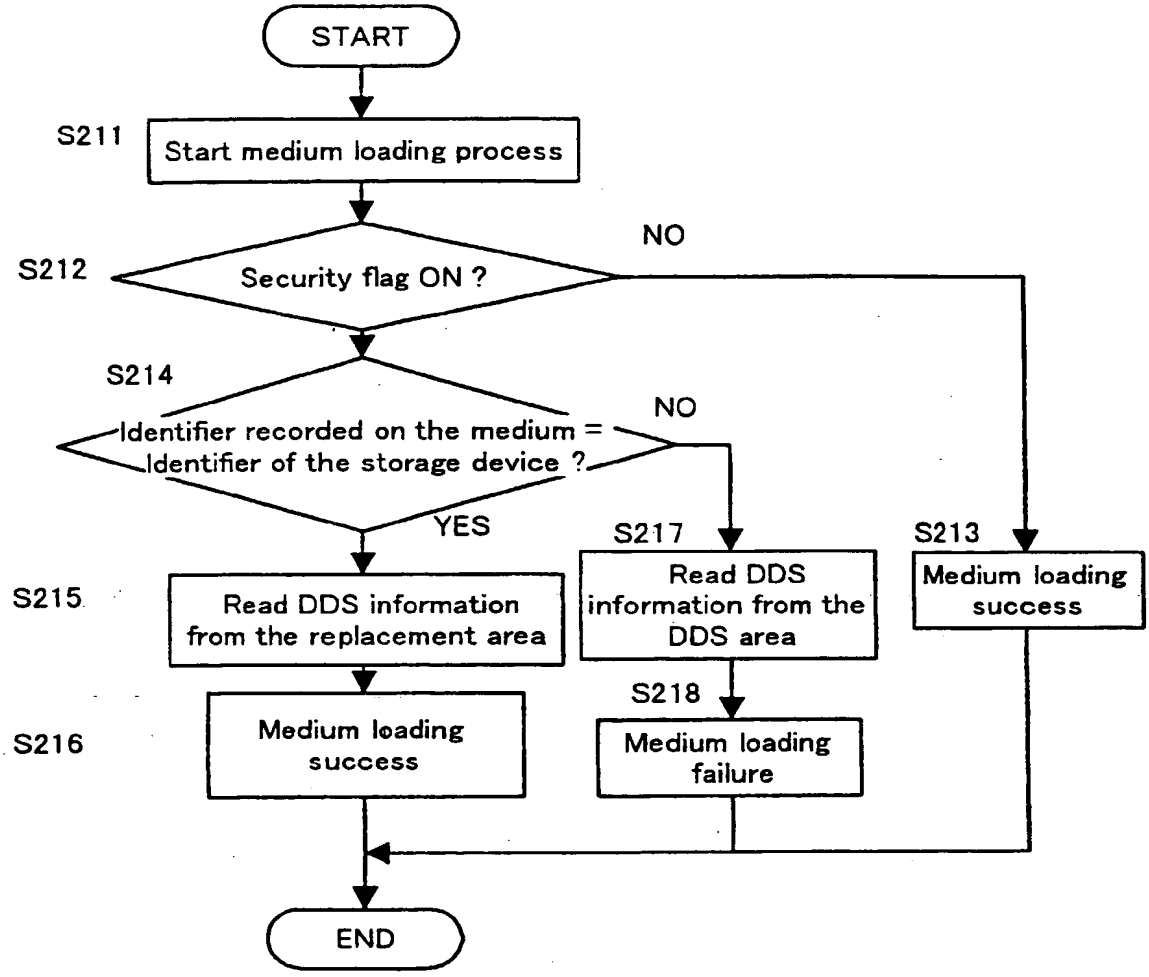


FIG. 10

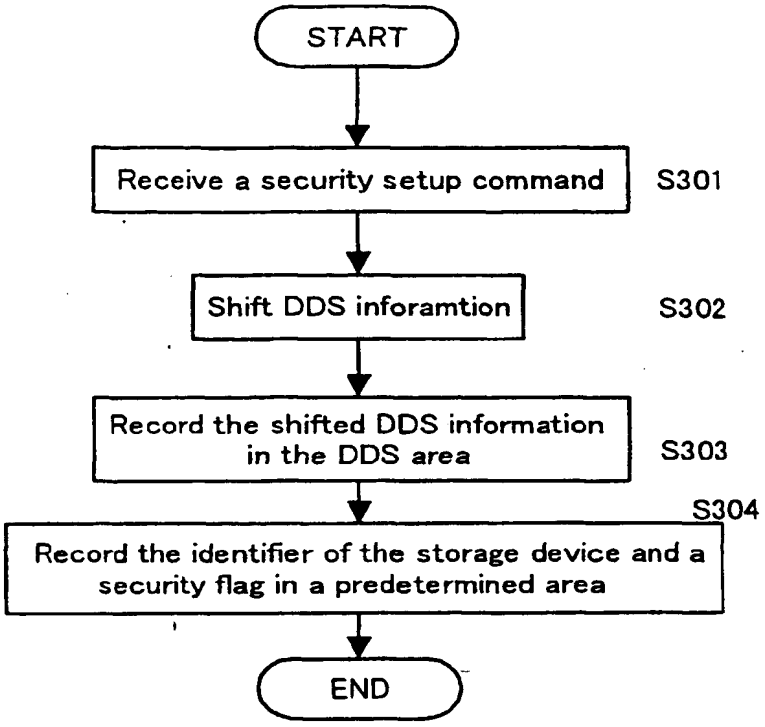


FIG. 11

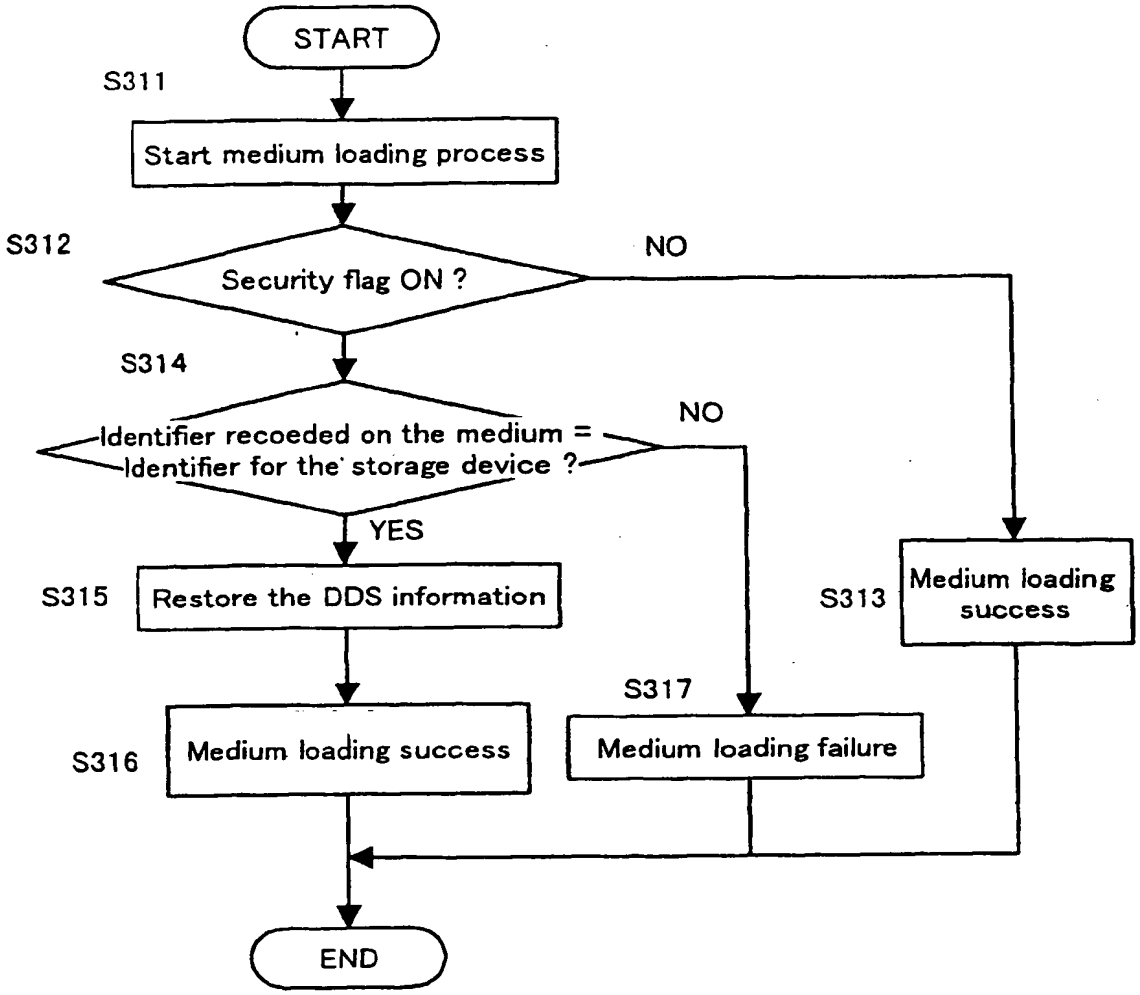


FIG. 12

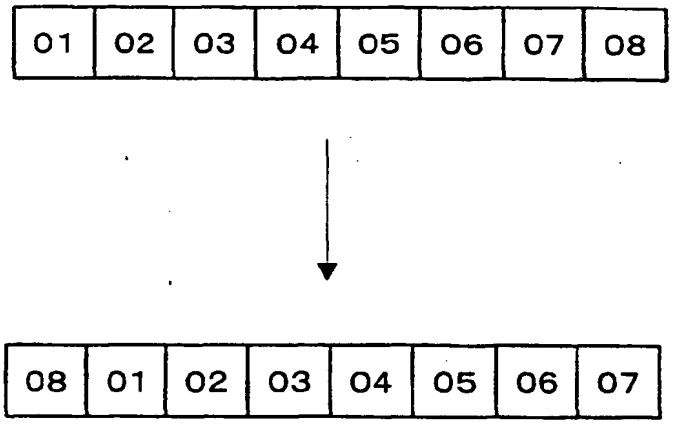


FIG. 13

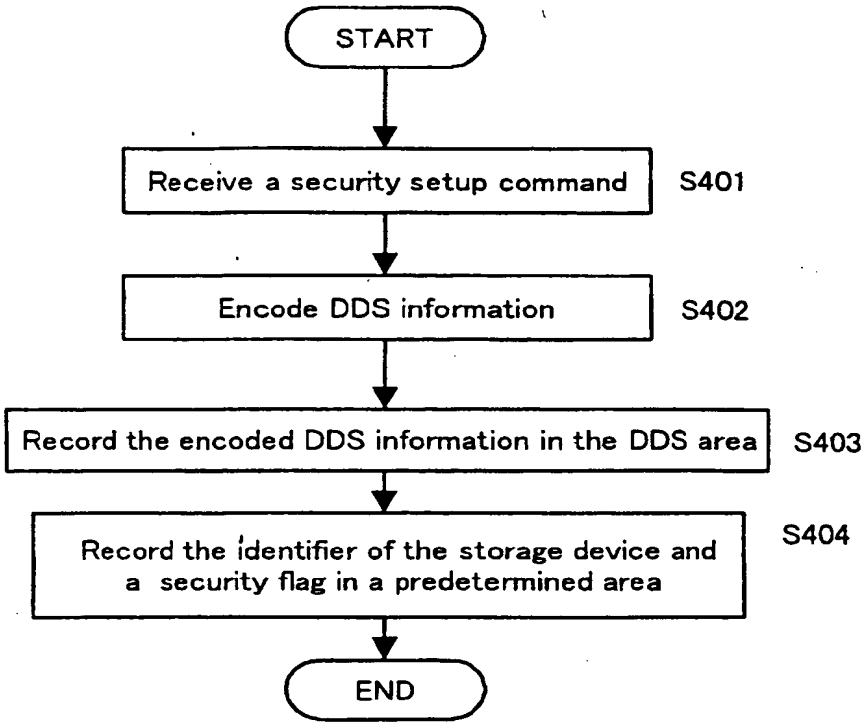


FIG. 14

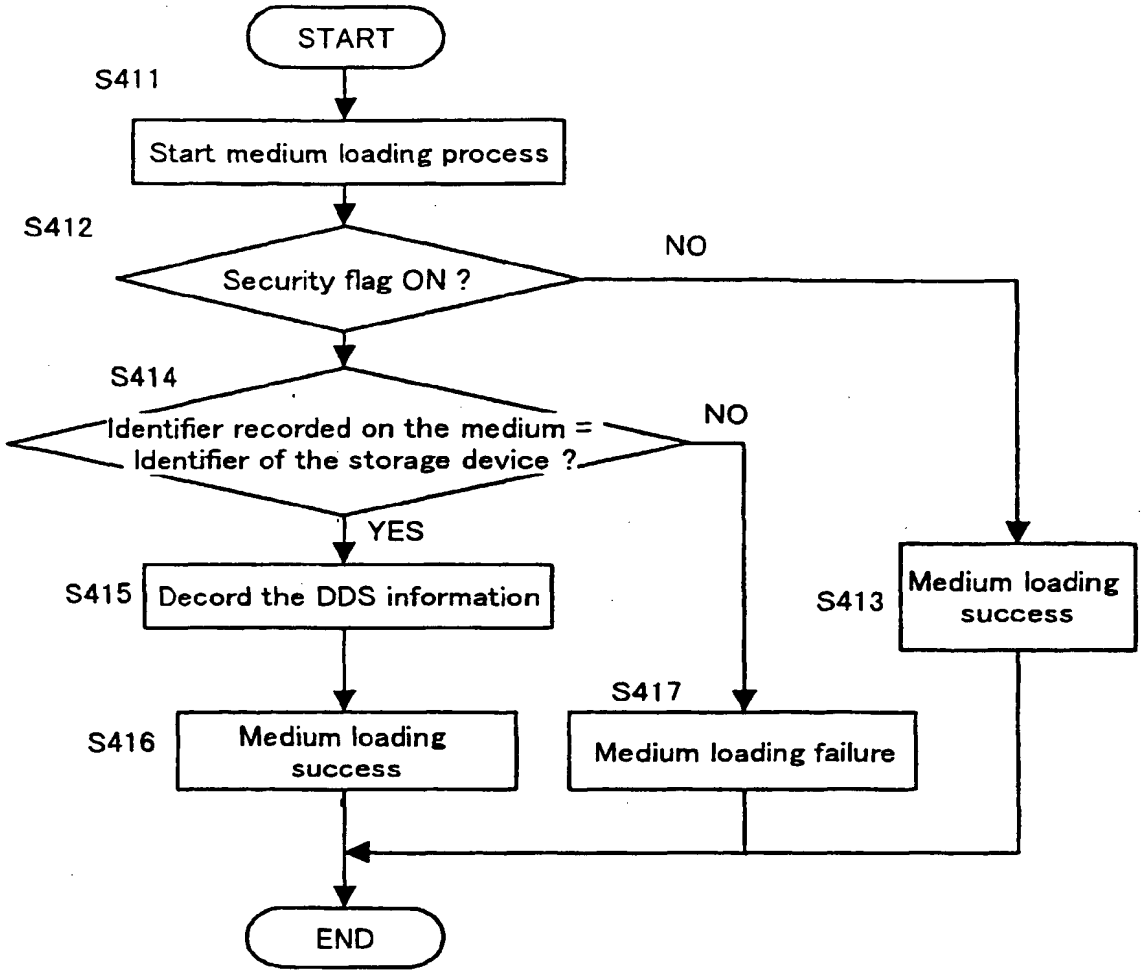


FIG. 15

		Bit							
		7	6	5	4	3	2	1	0
Byte	00	0	0	0	0	0	1	0	0
	01	LUN			FMT DATA	CMP LIST	DEFECT LIST FORMAT		
	02	Security level							
	03	INTERLEAVE							
	04	INTERLEAVE							
	05	0	0	0	0	0	0	Flag	Link

FIG. 16

		Bit							
		7	6	5	4	3	2	1	0
Byte	00	1	1	1	0	0	0	0	0
	01	LUN			0	0	0	0	0
	02	Security level							
	03	X'00'							
	04	Parameter list length							
	05	0	0	0	0	0	0	Flag	Link

FIG. 17A

Bit / Byte	7	6	5	4	3	2	1	0
0	X' 00'							
1	X' 00'							
2	X' 00'					Write address information	Read address information	LBASFT
3	Data block length							

FIG. 17B

Bit / Byte	7	6	5	4	3	2	1	0
0	Security level							
1	Page code							
:	Parameter field							
n								

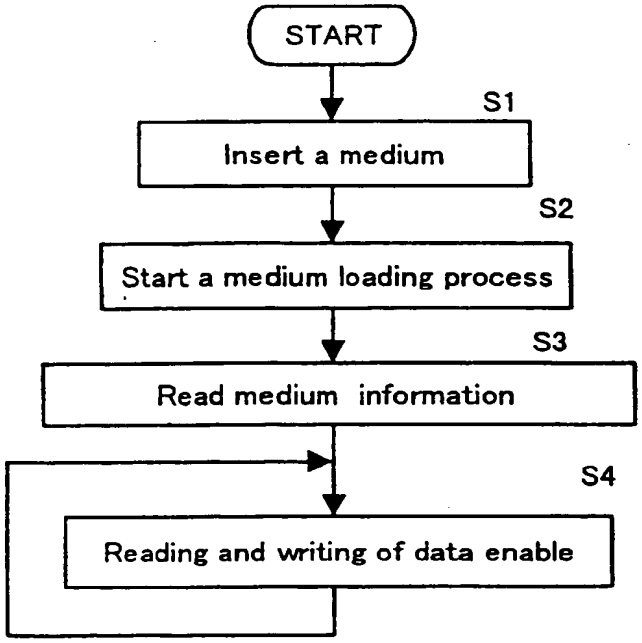
FIG. 18A

Bit / Byte	7	6	5	4	3	2	1	0
0	X'01'							
1	X'01'							
2~22	Password							

FIG. 18B

Bit / Byte	7	6	5	4	3	2	1	0
0	X'01'							
1	X'02'							
2	Page length							
3~6	Security LBA							
. .	Security LBA							
n~n+3	Security LBA							

FIG. 19



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 930 615 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
15.12.1999 Bulletin 1999/50

(43) Date of publication A2:
21.07.1999 Bulletin 1999/29

(21) Application number: **98112212.0**

(22) Date of filing: **02.07.1998**

(51) Int. Cl.[6]: **G11B 20/10**, G11B 27/28

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **20.01.1998 JP 891598**

(71) Applicant: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

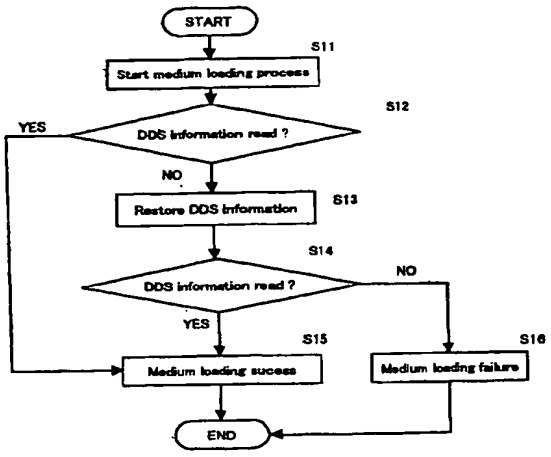
(72) Inventors:
- **Yamakawa, Teruji,**
  c/o Fujitsu Program Lab. Ltd.
  Yokohama, 222-0033 (JP)
- **Imamura, Kiyomi,**
  c/o Fujitsu Limited
  Kawasaki-shi, Kanagawa 211-8588 (JP)

(74) Representative:
Seeger, Wolfgang, Dipl.-Phys.
SEEGER & SEEGER
Patentanwälte & European Patent Attorneys
Georg-Hager-Strasse 40
81369 München (DE)

(54) Data storage device and control method therfor

(57) It is provided a data storage device which reads data from and/or writes data to a memory medium, comprising: an acquisition unit for acquiring management information which is recorded by a predetermined form in said memory; and a controller for converting the management information into an another form. The controller rearranges the management information to convert the management information into another form, and also the controller restores the converted management information to the predetermined form according to a relationship between a first identifier recorded on the memory medium and a second identifier recorded in the data storage device. When, for example, the two identifiers match, the acquisition unit can acquire the management information, and the reading and writing of data is enabled. When the two identifiers do not match, restoration of the management information to a predetermined form is not effected, so that the acquisition unit can not acquire the management information and the reading and writing of data is disabled.

FIG. 4



EP 0 930 615 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 11 2212

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	US 5 124 963 A (ANDO RYO) 23 June 1992 (1992-06-23) * the whole document *	1,16,18, 23	G11B20/10 G11B27/28
A	EP 0 818 748 A (MURAKOSHI HIROMASA) 14 January 1998 (1998-01-14) * abstract * * column 7, line 37 - line 51 * * figure 3 *	1,16,18, 23	
A	EP 0 773 490 A (FUJITSU LTD) 14 May 1997 (1997-05-14) * abstract * * column 1, line 3 - column 2, line 38 * * column 4, line 46 - column 5, line 5 * * column 5, line 30 - column 7, line 10 * * figures 1,4,6,7 *	1-5,9, 12-24	
A	EP 0 553 545 A (SEGA ENTERPRISES KK) 4 August 1993 (1993-08-04) * abstract * * column 4, line 9 - column 5, line 51 * * figures 1-3 *	1,16,18, 23	TECHNICAL FIELDS SEARCHED (Int.Cl.6) G11B
A	US 5 644 444 A (BRAITHWAITE DAVID G ET AL) 1 July 1997 (1997-07-01) * abstract * * column 2, line 24 - column 3, line 2 * * column 7, line 58 - column 12, line 7 * * figures 6A,6B *	1,16,18, 23	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	26 October 1999	Barel-Faucheux, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 11 2212

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	EP 0 813 194 A (SONY CORP) 17 December 1997 (1997-12-17) * abstract * * column 16, line 39 - column 17, line 28 * * column 19, line 25 - column 20, line 31 * * column 20, line 43 - line 46 * * column 23, line 49 - column 25, line 3 * * column 25, line 27 - line 31 * * figures 1,6-8 *	1,16,18, 23	
A	EP 0 439 290 A (SONY CORP) 31 July 1991 (1991-07-31) * abstract * * column 24, line 32 - column 25, line 22 * * column 27, line 20 - line 23 * * column 28, line 11 - line 59 * * column 29, line 12 - line 26 * * figures 14,16-18 *	1,16,18, 23	TECHNICAL FIELDS SEARCHED (Int.Cl.6)
A	US 5 379 433 A (YAMAGISHI TORU) 3 January 1995 (1995-01-03) * abstract; figure 4 *	1,16,18, 23	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	26 October 1999	Barel-Faucheux, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 11 2212

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

26-10-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5124963 A	23-06-1992	JP 2000332 C	08-12-1995
		JP 7031901 B	10-04-1995
		JP 63222379 A	16-09-1988
		AT 95940 T	15-10-1993
		CA 1306804 A	25-08-1992
		DE 3884829 D	18-11-1993
		DE 3884829 T	10-02-1994
		EP 0281415 A	07-09-1988
		HK 119695 A	28-07-1995
		KR 9700688 B	18-01-1997
EP 0818748 A	14-01-1998	JP 2810033 B	15-10-1998
		JP 10083298 A	31-03-1998
		AU 2844497 A	15-01-1998
		CA 2209596 A	08-01-1998
		US 5943650 A	24-08-1999
EP 0773490 A	14-05-1997	JP 9134311 A	20-05-1997
		JP 9134330 A	20-05-1997
		US 5857021 A	05-01-1999
EP 0553545 A	04-08-1993	JP 2942837 B	30-08-1999
		JP 5210497 A	20-08-1993
		EP 0718838 A	26-06-1996
		US 5371792 A	06-12-1994
		US RE35839 E	07-07-1998
US 5644444 A	01-07-1997	CA 2211590 A	19-09-1996
		DE 789908 T	19-02-1998
		EP 0789908 A	20-08-1997
		JP 10504420 T	28-04-1998
		WO 9628820 A	19-09-1996
		US 5949601 A	07-09-1999
EP 0813194 A	17-12-1997	JP 10003745 A	06-01-1998
		CN 1182268 A	20-05-1998
EP 0439290 A	31-07-1991	JP 3215891 A	20-09-1991
		JP 2805102 B	30-09-1998
		JP 3286444 A	17-12-1991
		DE 69122632 D	21-11-1996
		DE 69122632 T	13-03-1997
		US 5361173 A	01-11-1994
US 5379433 A	03-01-1995	JP 2293930 A	05-12-1990

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82